



אוקטובר 2025  
חשוון תשפ"י

## הפיקוח על מגמת תקשוב

טכנאים/הנדסאים תקשוב. סמל מגמה: 35.91  
הנחיות ודגשים לחומר הלימוד לבחינות גמר, טכנאים והנדסאים – מועד אביב תשפ"א, 2026  
עמוד: 10

הערות	בחינה בכתבה	משך בחינה בשעות	צורת הבחינה	שם שאלון	סמל שאלון
<b>חומר עזר:</b> מחשבבו פשוט שאיןו ניתן לתכנות ולא אפשר לחמיר ערכיהם בסיסי ספרה שונות. כל חומר עזר כתוב בכתב יד או מודפס על נייר.	י"ג	4	בכתב	רשותות תקשורת ואבטחת מידע	<b>735001</b>

עמודים 10-15

שימו לב ! החל ממועד זה הבחינה תהיה בכתב !!

### מבנה השאלון

- פרק ראשון – רשותות תקשורת

יש לענות על 18 מתוך 20 השאלות 20-1. כל שאלה = 2.5 נק'. סה"כ 45 נקודות

- פרק שני – אבטחת מידע

יש לענות על 22 מתוך 24 השאלות 44-21. כל שאלה = 2.5 נק'. סה"כ 55 נקודות

- סוגי שאלות בבחן :

- שאלות אמריקאיות
- שאלות השלמת משפטיים, השלמה מתוך מחזור מילימ
- שאלות נכון/לא נכון
- סימון משפטיים נכוןים לגבי טענות מסוימות

### תכנית לימודים ודגשים לבחינה - פרק ראשון – רשותות תקשורת – כיתה י"ג

הנושאים בבחינה על פי תכנית הלימודים בקישור : [מערכות תקשוב יי"ג תכנית לימודים – מערכות תקשורת](#)

פירוט הנושאים	הפרקים בתוכנית הלימודים
<p>כל הפרק.</p> <p> חוזרת כללית על הנושאים שנלמדו בתיכון. בדגש על :</p> <ul style="list-style-type: none"> <li>- ייצוג והמרת מספרים בינאריים-עשרוני-הקסדימלי</li> <li>- מודל הרשת OSI – להתמקד בשכבות 1,2,3</li> <li>- מבנה חבילת Ethernet (layer 2 &amp; 3) Destination And Source Address</li> <li>- ההבדלים בין TCP UDP לבין</li> <li>הבנייה מושגים :</li> <ul style="list-style-type: none"> <li>- connection-oriented protocol, connectionless protocol</li> <li>- ip nat inside .... overload - NAT</li> <li>- פרוטוקול ARP (הפקודה arp –a, arp request, arp reply)</li> <li>- הגדרות בסיסיות בהתקני רשת (נתב, מטג, הגדרות סיסמאות)</li> </ul> <p>ACL - סטנדרטי ומורחב (כולל לחסום/לאפשר פורטים)</p> <p>- פקודות CLI שנכתבות ב-Mode הנכו</p> </ul>	1 - מבוא למערכות תקשורת

אוקטובר 2025

חשון תשפ"י

## הפיקוח על מגמת תקשוב

טכנאים/הנדסאים תקשוב. סמל מגמה: 35.91

עמוד: 11

הנחיות ודגשים לחומר הלימוד לבחינות גמר, טכנאים והנדסאים – מועד אביב תשפ"א, 2026

כל הפרק	2 - חיבור לאינטרנט באמצעות ISP
כל הפרק. דגש על IPv4: מרחב כתובות של 32 סייביות מחלקות ● חלק רשות חלק לקוח - subnetting ● מסכת רשות משנה (CIDR) ● כתובות IP מיעוזות ● כתובות IP פרטיות וציבוריות, ping,icmp ● APIPA ● localhost ● IPv6	3 - כתובות רשת
כתובת IPv6 של MAC ● יישום כתובת IPv6unicast ● הגדרת כתובות unicast ● הגדירה דינמית של כתובת unicast ● כתובות Link-Local ● יצירת כתובות Link-Local ע"ג נתבים ● ניתוב IPv6 עם כתובות Link-Local בלבד. ● כתובות IPv6 multicast מסוג multicast ● טווח כתובות מוקומי של multicast ●	
כל הפרק – דגש על ה프וטוקולים וסוגי השירותים : SMT P,FTP ,SSH ,HTTP ,HTTPS ,SNMP ,TFTP DORA, ipconfig/release – DHCP – תהליך הבנת התהיליך וסוגי שירות שידור	4 – פקודות ושירותי רשת

אוקטובר 2025

חשון תשפ"י

## הפיקוח על מגמת תקשוב

טכנאים/הנדסאים תקשוב. סמל מגמה: 35.91

עמוד: 12

הנחיות ודגשים לחומר הלימוד לבחינות גמר, טכנאים והנדסאים – מועד אביב תשפ"א, 2026

<ul style="list-style-type: none"> <li>• יצירת VLAN-ים במתג</li> <li>• שיקן משקיקים ל- VLAN-ים (משקיק ACCESS)</li> <li>• חיבור בין מתגים - משקיק TRUNK</li> <li>• פרוטוקול DTP</li> <li>• native VLAN</li> <li>• VLAN pruning</li> <li>• default VLAN</li> <li>• ניתוב בין VLAN-ים</li> <li>• router on a stick</li> <li>• layer 3 switch</li> <li>• פרוטוקול VTP</li> <li>• VTP modes</li> <li>• VTP Domain</li> <li>• VTP password</li> <li>• VTP pruning</li> <li>• פרוטוקול STP</li> <li>• יתירות ברשות מקומית</li> <li>• תקנים שונים של STP           <ul style="list-style-type: none"> <li>◦ STP 802.1D</li> <li>◦ IEEE 802.1W - RSTP</li> </ul> </li> <li>• BPDU</li> <li>• STP port states</li> <li>• bridge ID</li> <li>• root bridge election (link cost)</li> <li>• bpdu guard, bpdu filter</li> <li>• root guard</li> <li>• PVST (per VLAN spanning-tree)</li> <li>• RPVST (Rapid per VLAN spanning-tree)</li> </ul>	<p>6 - מיתוג ברשות מקומית</p>
<ul style="list-style-type: none"> <li>•DHCP : DHCP on DHCP Relay Agent על נתב, הגדרת הגדרת DHCP על נתב, הגדרת stick,</li> <li>•רשימות גישה ACL: רשימת גישה סטנדרטית, רשימת גישה מורחבת הגדרת Wildcard mask</li> <li>•נתבים : CLI, ISR, משקקים, הקצאת כתובות IPv4 לממשק, TTL (Time to Live)</li> <li>•שיטות חיבור בין נתבים: point-to-point, point to multipoint, Virtual-link</li> </ul>	<p>7 - מבוא לרשת רחבה WAN</p>
<ul style="list-style-type: none"> <li>• ניתוב : תהליכי ניתוב, כתובות ARP ,default gateway, ניתוב סטטי, RIPv2, IGP, Distance Vector Messages, Split Horizon, Administrative Distance, Summarization</li> <li>• מבנה טבלת הניתוב</li> <li>• רשותות המחברות באופן ישיר/רשותות מרוחקות</li> <li>• הובלה של מנוגות (packets) לרשותות המחברות באופן ישיר לנtb (ARP)</li> <li>• ניתוב סטטי</li> <li>• ניתוב בירית מחדל (סטטי)</li> <li>• פרוטוקולי ניתוב דינמיים פנים ארגוניים (IGP)           <ul style="list-style-type: none"> <li>◦ distance vector</li> <li>◦ link state</li> <li>◦ (משולב) hybrid</li> </ul> </li> </ul>	<p>8 – פרוטוקולים לניתוב ברשת רחבה</p>

אוקטובר 2025

חשון תשפ"י

**הפיקוח על מגמת תקשוב****טכנאים/הנדסאים תקשוב. סמל מגמה: 35.91**

עמוד: 13

הנחיות ודגשים לחומר הלימוד לבחינות גמר, טכנאים והנדסאים – מועד אביב תשפ"א, 2026

<ul style="list-style-type: none"> <li>• פרוטוקול ניתוב RIP</li> <li>• גרסה 2 (הבדלים בין גרסה 1 ל 2)</li> <li>• פרסום רשותות (הפעלת RIP על ממשק הנטב)</li> <li>• חישוב סכימת רשותות וביטול סכימה אוטומטית</li> <li>• ממשקים פסייביים</li> <li>• מגנונים למניעת לולאות ניתוב</li> <li>• הפקת נתיב ברירת מחדל .Administrative distance</li> <li>• עליות הנתיבים (metric)</li> <li>• פרוטוקול OSPF (AS,ASBR,DR,BDR,LSAs)</li> <li>• פרוטוקול EIGRP</li> <li>• פרוטוקול IGRP</li> <li>• פרוטוקול BGP</li> <li>• להבין היטב את כל המרכיבים בטבלת הניתוב - show ip route</li> </ul>		
<p>פרוטוקולים לניהול התקני רשות</p> <ul style="list-style-type: none"> <li>• syslog</li> <li>○ משלוח הודעות בזמן אמת למשתמשים</li> <li>○ אחסון הודעות יומן המערכת (log) לעיון מאוחר יותר</li> <li>○ בניית הודעת יומן המערכת</li> <li>○ רמות חרمرة של הודעות יומן המערכת</li> <li>○ הגדרה ואיומות של פעילות יומן המערכת</li> <li>○ פקודות Debug ווימני המערכת</li> <li>○ NTP</li> <li>○ הגדרת זמן ואזור זמן</li> <li>○ יישום לקוחות, שירותים ומצב שרת/לקוח ב-NTP</li> <li>○ שימוש במשק מסוג Loopback</li> </ul>		9 – ניהול רשות מתקדם

**פרק שני – אבטחת מידע****סוגי שאלות ב מבחון :**

- שאלות אמריקאיות
- שאלות שלמת משפטים, שלמות מתוך מחסן מילימ
- שאלות נכון/לא נכון

**תכנית לימודים ודגשים לבחינה – פרק שני – אבטחת מידע – ביתה י"ג**תוכנית הלימודים – אבטחת מידע – ביתה י"ג

אוקטובר 2025  
חשוון תשפ"ה

## הפיקוח על מגמת תקשוב

טכנאים/הנדסאים תקשוב. סמל מגמה: 35.91

עמוד: 14

הנחיות ודגשים לחומר הלימוד לבחינות גמר, טכנאים והנדסאים – מועד א' אביב תשפ"א, 2026

פירוט הנושאים	הפרקים בתוכנית הלימודים
<ul style="list-style-type: none"> <li>• מבוא לאיוומי רשות</li> <li>• עקרונות אבטחת הרשות</li> <li>• אביזרים לאבטחת רשות וסטנדרטים באבטחה</li> <li>• ארגון אבטחת הרשות</li> <li>• תחום אבטחת המידע</li> <li>• CIA מודל</li> <li>• התמודדות מול וירוסים סועסים טרויאניים ותולעים</li> <li>• חקר ההתקפות, סוגים נזקיפים / איוומיים (External Attacker) (איום פנים ארגוני), תוקף חיצוני (Insider Threats)</li> <li>• סוגים נוספים</li> <li>• איסוף מידע על התקפות</li> <li>• התקפת מערכות גישה</li> <li>• התקפת מערכות ע"י מניעת שירות DDOS, DOS, Phishing, Brute force, Spear phishing, Man-in-the-Middle, SQL injection</li> <li>• DHCP starvation attack, DHCP spoofing</li> <li>• DHCP Offer (Rough)</li> <li>• Show ip dhcp binding</li> <li>• ARP spoofing</li> <li>• שיכון מתקפות ברוטליות</li> </ul>	פרק 1 – מבוא לאיוumi רשות חדשים
<ul style="list-style-type: none"> <li>• אבטחת נתבי קצה</li> <li>• ניהול והגדרת חיבורים מרוחקים</li> <li>• הגדרת SSH לגישה מרוחיק</li> <li>• הגדרות רמות גישה</li> </ul>	פרק 2 – אבטחת אביזרי רשות
<ul style="list-style-type: none"> <li>• מודל AAA</li> <li>• שרתיים מבוססי מודל ה AAA</li> <li>• הגדרת שרתי TACACS + עם מפתחות מוצפנים,</li> <li>• זיהוי פורטים, הגדרות משתמשים</li> <li>• הגדרת שרתי RADIUS עם מפתחות מוצפנים, זיהוי פורטים</li> <li>• אבטחת נתבי קצה</li> </ul>	פרק 3 – מודל ה AAA
<ul style="list-style-type: none"> <li>• הגדרת ACLs סטנדרטי ומורחב במשקי CLI</li> <li>• שימושACL לשיטות גישה לשרת +RADIUS, TACACS</li> <li>• יצירת מניעת התקפות על ידי ACLs במערכות ACLs לרבות Network Access Control List Stateless and Stateful Firewall Filters</li> <li>• אבטחת הרשות על ידי חומות אש</li> </ul>	פרק 4 – הגנה על הרשות ושליטה בת慮ורת הנתונים
<ul style="list-style-type: none"> <li>• מאפייני מערכות IDS ו IPS והבדלים בبنיהם</li> <li>• מערכות מבוססות רשות חתימות IPS (Host Intrusion Prevention System) HIPS , IPS (Network Intrusion Prevention System) NIPS</li> <li>• מאפייני חתימת IPS , אזעקה IPS</li> <li>• ניתור ופתרון תקלות במערכות IDS ו IPS</li> </ul>	פרק 5 – מניעת חדירה לרשות המקומית והרשות הרחבה
<ul style="list-style-type: none"> <li>• מערכות קצה לאבטחת הרשות</li> </ul>	פרק 6 – אבטחת הרשות המקומית

אוקטובר 2025

חשוון תשפ"ה

**הפיקוח על מגמת תקשוב****טכנאים/הנדסאים תקשוב. סמל מגמה: 35.91**

עמוד: 15

הנחיות ודgeshim לחומר הלימוד לבחינות גמר, טכנאים והנדסאים – מועד אביב תשפ"ה, 2026

<ul style="list-style-type: none"> <li>• מערכות לאבחן מיילים, אתרים, אבטחה</li> <li>• הכוורת עם אבטחה בשכבות העורק (Link Data)</li> <li>• BPDU Guard</li> <li>• התקפות על מערך ה LAN</li> <li>• התקפות מתקדמות ב VLAN</li> <li>• התקפות על מערכי VLAN</li> </ul> <p>Switch Spoofing VLAN Attacks, VLAN hopping attack Switch(config)# ip dhcp snooping ....</p> <ul style="list-style-type: none"> <li>• מוצבי אבטחה בשכבות העורק והתמודדות עם התקפות</li> <li>• הגדרת מוצב אבטחה (SC) (Control Storm)</li> <li>• (Switch Port Analyzer) SPAN</li> <li>• והדרכת SPAN</li> <li>• ואבטוח באמצעות SPAN</li> <li>• שילוב SPAN עם IDS ליצירת מראה רשת</li> </ul>	
<ul style="list-style-type: none"> <li>• תורת הצפנה</li> <li>• חתימה דיגיטלית(Digital Signature)</li> <li>• צפינים שונים וסוגי הצפנות קדומות</li> <li>• התקפות ברוטליות לפותיחת צפינים</li> <li>• חוקי NSA לגבי הצפנות מידע</li> <li>• סוגי הצפנה ופרוטוקולי הצפנה, אוטנטיקציה וסודיות הצפנות על ידי Hashing</li> <li>• אלגוריתם הצפנה AES, RSA, DES</li> <li>• Hashing 5-MD</li> <li>• ניהול מפתחות על ידי שינוי אחסון וריפיקציה משתנה</li> <li>• מפתחות ארוכים ומפתחות קצרים</li> <li>• הצפנות סימטריות ו-א-סימטריות</li> <li>• אלגוריתם Diffie-Hellman</li> <li>•DSA אלגוריתמים לחתימות דיגיטליות</li> <li>• סטנדרטים של PKI וסטנדרטים אישור סטנדרטים</li> </ul>	<p>פרק 7 – שיטות הצפנה</p>
<ul style="list-style-type: none"> <li>• VPN שימושו בחברה ובארגוני</li> <li>• פתרונות לקוח VPN חיבור מרוחק צד לקוח</li> <li>• היכרות עם סטנדרט IPSec מערכות IPSec והטמעת IPSec יתרוןות וחסרונות</li> <li>• ההדרת VPN על ידי טופולוגיה אתר לאתר协议 isakmp על בסיס CLI</li> <li>• בדיקת VPN ויצירת מערכת שליטה לבקרה לפתרון בעיות</li> </ul>	<p>פרק 8 – VPN – מערכת (Virtual Private Network)</p>
<ul style="list-style-type: none"> <li>• בדיקת אבטחת הרשות</li> <li>• ניהול סיכונים וניהול פגיעות תוך חברתיות</li> <li>• הימנענות מסיכונים ובידוד התקפות</li> <li>• בדיקת פגיעות על ידי כלים שונים</li> <li>• בדיקת פגיעות על ידי NMAP</li> </ul>	<p>פרק 9 - ניהול אבטחת רשות מתקדם</p>

**\*\*\* סוף שאלון 1001 \*\*\***